What Is Claimed Is:

1. In a multi-stage intrusion detection system, a method of detecting a plurality of intrusion attacks to a packet transmitted on a network, the intrusion attacks associated with a plurality of conditions, the method comprising:

receiving the packet;

determining at a first stage of the intrusion detection system whether a first condition assigned to the first stage is satisfied for the packet;

determining at a second stage of the intrusion detection system whether a second condition assigned to the second stage is satisfied for the packet; and

determining that the packet corresponds to an intrusion attack when it is determined that the first condition and the second condition are satisfied.

2. The method of claim 1, wherein responsive to determining that the packet corresponds to an intrusion attack, the method further comprises taking an action for the intrusion attack.

3. The method of claim 2, wherein the action comprises warning that the intrusion attack occurred.

4. The method of claim 1, wherein determining at a first stage whether a first condition is satisfied comprises:

responsive to the first condition being satisfied, adding an indication to the packet representing that the first condition is satisfied.

5. The method of claim 4, wherein determining that the packet corresponds to an intrusion attack comprises determining that the indication is added and that the second condition is satisfied.

6. The method of claim 1, wherein the network is the Internet and the packet is an IP packet.

7. An intrusion detection system for detecting a plurality of intrusion attacks to a packet transmitted on a network, each intrusion attack associated with a plurality of conditions, each condition belonging to one of a first, second, third, fourth and fifth set of conditions, the intrusion detection system comprising:

a generic extension builder for (i) receiving the packet, (ii) processing the first set of conditions on the packet to generate generic extensions, and (iii) outputting the packet along with the generic extensions added to the packet;

a session cache module coupled to the generic extension builder for (i) receiving the packet with the generic extension, (ii) processing the second set of conditions on the packet to generate session cache extensions, and (iii) outputting the packet along with the generic extensions and the session cache extensions added to the packet;

an application decode module coupled to the session cache module for (i) receiving the packet with the generic extensions and the session cache extensions, (ii) processing the third set of conditions on the packet to generate application decode extensions, and (iii) outputting the packet along with the generic extensions, the session cache extensions, and the application decode extensions added to the packet;

a rule engine module coupled to the application decode module for (i) receiving the packet with the generic extensions, the session cache extensions, and the application decode extensions; (ii) processing the fourth set of conditions on the packet to generate rule engine extensions, and (iii) outputting the packet along with the generic extensions, the session cache extensions, the application decode extensions, and the rule engine extensions added to the packet; and

an intrusion detection policy engine coupled to the rule engine module for (i) receiving the packet with the generic extensions, the session cache extensions, the application decode extensions, and the rule engine extensions; (ii) processing the fifth set of conditions on the packet, (iii) determining whether all the conditions of an intrusion attack are satisfied based upon the generic extensions, the session cache extensions, the application decode extensions, the rule engine extensions, and the processed fifth set of conditions, (iv)

taking an action corresponding to the determined intrusion attack, and (v) outputting the packet.

8. The intrusion detection system of claim 7, further comprising a policy manager controlling the application decode module, the rule engine module, and the intrusion detection policy engine, wherein:

the application decode module receives application decode data from the policy manager for use in processing the third set of conditions on the packet;

the rule engine module receives the fourth set of conditions from the policy manager; and

the intrusion detection policy engine receives the fifth set of conditions from the policy manager.

9. A multi-stage intrusion detection system for detecting a plurality of intrusion attacks to a packet transmitted on a network, each intrusion attack associated with a plurality of conditions, the multi-stage intrusion detection system comprising:

a plurality of modules each corresponding to selected ones of the conditions and each determining whether the corresponding conditions are satisfied; and

a policy manager controlling selected ones of the modules and providing information used in determining whether the corresponding conditions are satisfied to the selected ones of the modules,

wherein an intrusion attack is detected when all the conditions corresponding to the intrusion attack are determined to be satisfied by the respective modules.

10. An intrusion detection system for detecting a plurality of intrusion attacks to a packet transmitted on a communication network, each intrusion attack associated with a rule having a plurality of conditions and an action to be taken when the intrusion attack is detected, the intrusion detection system comprising:

a rule database storing the rules for each of the intrusion attacks;

a policy compiler coupled to the rule database and converting the conditions in the rules to a rule tree, the rule tree including a plurality of condition node pairs each having an expression node and a value node, each condition node pair corresponding to one condition and coupled to another condition node pair via at least one branch to form a plurality of paths, such that traversing along one of the paths corresponds to determining the conditions of a rule associated with one of the intrusion attacks; and

an intrusion detection policy agent coupled to the policy compiler for determining whether an intrusion attack occurred to the packet based upon the rule tree provided by the policy compiler.

11. The intrusion detection system of claim 10, wherein a user provides the rule database with the rules for the intrusion attacks.

12. The intrusion detection system of claim 10, wherein the network is the Internet and the rules for the intrusion attacks are provided to the rule database by a website storing the rules.

13. The intrusion detection system of claim 10, wherein the policy compiler converts the conditions to the rule tree by grouping common conditions among the rules, each condition node pair in the tree corresponding to one of the common conditions or a non-common condition, and coupling a first condition node pair with a second condition node pair among the condition node pairs when both the first and second condition node pairs correspond to a same rule.

14. The intrusion detection system of claim 10, wherein a user selects a number of rules among the rules stored in the rule database and provides the selection of the rules to the policy manager, and the policy manager converts the conditions in only the selected rules to the rule tree.

15. The intrusion detection system of claim 10, wherein the intrusion detection policy agent comprises a plurality of modules each corresponding to selected ones of the condition node pairs and each determining whether the conditions corresponding to the selected ones of the condition node pairs are satisfied, wherein an intrusion attack is detected when all the conditions corresponding to the intrusion attack are determined to be satisfied by the respective modules.

16. The intrusion detection system of claim 15, further comprising a policy

manager controlling selected ones of the modules of the intrusion detection policy agent and providing information used for determining whether the conditions are satisfied to the selected ones of the modules.

17. The intrusion detection system of claim 15, wherein the conditions belong to one of a first, second, third, fourth, and fifth set of conditions, and the plurality of modules comprise:

a generic extension builder for (i) receiving the packet, (ii) processing the first set of conditions on the packet to generate generic extensions, and (iii) outputting the packet along with the generic extensions added to the packet;

a session cache module coupled to the generic extension builder for (i) receiving the packet with the generic extensions, (ii) processing the second set of conditions on the packet to generate session cache extensions, and (iii) outputting the packet along with the generic extensions and the session cache extensions added to the packet;

an application decode module coupled to the session cache module for (i) receiving the packet with the generic extensions and the session cache extensions, (ii) processing the third set of conditions on the packet to generate application decode extensions, and (iii) outputting the packet along with the generic extensions, the session cache extensions, and the application decode extensions added to the packet;

a rule engine module coupled to the application decode module for (i) receiving the packet with the generic extensions, the session cache extensions, and the application decode extensions; (ii) processing the fourth set of conditions on the packet to generate rule engine extensions, and (iii) outputting the packet along with the generic extensions, the session cache extensions, the application decode extensions, and the rule engine extensions added to the packet; and

an intrusion detection policy engine coupled to the rule engine module for (i) receiving the packet with the generic extensions, the session cache extensions, the application decode extensions, and the rule engine extensions; (ii) processing the fifth set of conditions on the packet, (iii) determining whether all the conditions of an intrusion attack are satisfied based upon the generic extensions, the session cache extensions, the application decode extensions, the rule engine extensions, and the processed fifth set of conditions, (iv) taking an action corresponding to the determined intrusion attack, and (v) outputting the packet.

18. The intrusion detection system of claim 17, wherein the policy manager controls the application decode module, the rule engine module, and the intrusion detection policy engine, and wherein:

the application decode module receives application decode data from the policy manager for use in processing the fifth set of conditions on the packet;

the rule engine module receives the fourth set of conditions from the policy manager; and

the intrusion detection policy engine receives the fifth set of conditions from the policy manager.

19. A computer-readable medium storing a rule tree for use in an intrusion detection system for detecting a plurality of intrusion attacks to a packet transmitted on a network, each intrusion attack associated with a rule having a plurality of conditions and an action to be taken when the intrusion attack is detected, wherein the rule tree comprises a plurality of condition node pairs each having an expression node and a value node, each condition node pair corresponding to one condition and coupled to another condition node pair via a branch to form a plurality of paths, such that traversing along one of the paths corresponds to determining all the conditions of the rule associated with one of the intrusion attacks.

20. The computer-readable medium of claim 19, wherein:

the rules include common conditions corresponding to more than one rule;

at least one of the condition node pairs in the tree corresponds to one of the common conditions; and

the condition node pairs are coupled to one another via branches when the coupled condition node pairs correspond to a same rule.

21. A multi-stage intrusion detection system for detecting a plurality of intrusion attacks to a packet transmitted on a network, the intrusion attacks associated with a plurality of conditions, the multi-stage intrusion detection system comprising:

a first stage receiving the packet and determining whether a first condition assigned to the first stage is satisfied for the packet; and

a second stage determining whether a second condition assigned to the second stage is satisfied for the packet,

wherein the multi-stage intrusion detection system determines that the packet corresponds to an intrusion attack when it is determined that the first condition and the second condition are satisfied.

22. The multi-stage intrusion detection system of claim 21, wherein responsive to determining that the packet corresponds to an intrusion attack, the multi-stage intrusion detection system takes an action for the intrusion attack.

23. The multi-stage intrusion detection system of claim 22, wherein the action comprises warning that the intrusion attack occurred.

24. The multi-stage intrusion detection system of claim 21, wherein responsive to the first condition being satisfied, the first stage adds an indication to the packet representing that the first condition is satisfied.

25. The multi-stage intrusion detection system of claim 24, wherein the second stage determines that the packet corresponds to an intrusion attack by determining that the indication is added and that the second condition is satisfied.

26. The multi-stage intrusion detection system of claim 21, wherein the network is the Internet and the packet is an IP packet.